REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

I. DOUBLE PATENTING

The Examiner submits that claims 7 and 9 of the present Application conflict with claims 1 and 3 of co-pending, commonly assigned U.S. Patent Application Serial No. 09/944,788 (hereinafter "the '788 Application"). The Examiner requests that the conflicting claims be cancelled from either the present application or from the '788 Application, in accordance with 37 CFR §1.78(b). The Applicants respectfully disagree with the Examiner's assertion.

In particular, the Applicants submit that claims 1 and 3 of the '788 Application recite additional limitations not recited in the present application. Specifically, claim 1 of the '788 Application recites the limitation of "updating a minimum similarity requirement for one or more features" of an alert or an alert class. This limitation is not recited in claim 7 or in claim 9 of the present Application. Likewise, the limitation of "rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value", as recited in claim 3 of the '788 Application, is not recited in claim 7 or in claim 9 of the present Application.

Thus, the Applicants respectfully submit that claims 7 and 9 of the present Application are patentably distinct from claims 1 and 3 of the '788 Application. Accordingly, the Applicants submit that neither claims 7 and 9 of the present Application nor claims 1 and 3 of the '788 Application need be cancelled under 37 CFR §1.78(b).

II. REJECTION OF CLAIMS 1-2 AND 4-9 UNDER 35 U.S.C. § 102

1. Claims 1, 2, 4 and 5

Claims 1, 2, 4 and 5 stand rejected as being anticipated by the Ziese patent (U.S. 6,484,315, issued November 19, 2002, hereinafter "Ziese"). The Applicants respectfully

disagree with the rejection. Nevertheless, the Applicants have clarified independent claim 1, from which claim 2 depends, in order to more clearly recite aspects of the present invention.

Ziese teaches a method for distributing intrusion detection updates in a network. In particular, Ziese teaches intrusion detection sensors that run programs for detecting intrusions based on "signatures" or patterns of known intrusions. In order to ensure recognition of the most current known intrusions, an intrusion detection sensor downloads an update containing new intrusion signatures from a server and locally installs the update. If the intrusion detection sensor is able to operate properly with the installed update, the intrusion detection sensor distributes the update to other intrusion detection sensors, who likewise install the updates.

The Examiner's attention is directed to the fact that Ziese fails to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, where the belief state indicates a state of a system resource or service and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claims 1, 4 and 5. Specifically, Applicants' claims 1, 4 and 5 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor information about the second sensor's belief state, said belief state indicating a state of at least one system resource or service; and

(b) adjusting a prior belief state of the first sensor, said belief state indicating a state of at least one system resource or service, the adjustment based at least in part on the second sensor's belief state. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding an apparent normal, degraded or compromised state of a monitored resource; and

(b) adjusting a prior belief state of the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm. (Emphasis added)

5. A method for enhancing the sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first and second sensors each maintaining belief over a number of possible states of the system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of the belief of the second sensor regarding the existence or validity of services supported on monitored computer system resources; and

(b) adjusting a prior belief state of the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious. (Emphasis added)

Nowhere does Ziese teach or even suggest the desirability of adjusting a belief state of a sensor relating to a state of a monitored system resource or service supported thereon, based on a belief state of another sensor. As described in the Applicants' specification, a first sensor in an intrusion detection system may maintain a belief state reflecting a current observation that indicates some condition or state of a system resource or service. By transmitting a second sensor's belief state (which may be based on a different observation) to the first sensor, the first sensor's belief state may be adjusted to increase the overall sensitivity of the intrusion detection system and to reduce false alarms (*See*, for example, page 5, lines 11-15). For example, a first sensor that observes network resources may detect that a server is malfunctioning. This belief state may be transmitted to a second sensor that observes network traffic, and the second sensor may then modify its belief state so that normal network traffic directed toward the malfunctioning server does not trigger a false alarm.

The portions of Ziese that the Examiner cites as allegedly teaching this limitation in fact only teach that sensors update their knowledge of intrusion signatures based on distributed updates from other sensors or servers. This is not the same as adjusting a belief state of a sensor regarding a state of a network resource or service. In other words, while the present invention claims updating a sensor's perception of a resource or service state (*e.g.*, normal, degraded, compromised, valid), Ziese teaches updating

the sensor's mechanisms for forming such a perception. Nowhere does Ziese teach, anticipate or suggest that the actual belief state of a sensor can be modified based on another sensor's belief state. Ziese thus fails to teach or anticipate a method in which a first sensor's belief state is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claims 1, 4 and 5. Therefore, the Applicants submit that independent claims 1, 4 and 5 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Ziese. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

2. Claims 6-9

Claims 6-9 stand rejected as being anticipated by the Kleinman patent (U.S. 6,128,640, issued October 3, 2000, hereinafter "Kleinman"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Kleinman fails to disclose or suggest the novel invention of organizing alerts into classes by evaluating a similarity between a new alert and an existing class of alerts, including adjusting or updating an expectation that feature values of the new alert and feature values of the existing alert class will match, as claimed in Applicants' independent claims 6, 7 and 9. Specifically, Applicants' claims 6, 7 and 9 positively recite:

6. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) comparing the new alert to one or more existing alert classes;

(c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(d1) associating the new alert with the existing alert class that the new alert

most closely matches; or

(d2) defining a new alert class that is associated with the new alert. (Emphasis added)

7. A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) receiving a new alert;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with one or more alert classes, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

9. A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert. (Emphasis added)

Nowhere does Kleinman teach or even suggest the desirability of grouping alerts into classes based on similar feature values, or adjusting or updating an expectation that feature values of a new alert and feature values of an existing alert class will match. As described in the Applicants' specification, the nature of an alert may affect a similarity expectation that indicates which features (*e.g.*, source IP address, destination IP address, type of attack, etc.) of the alert should be similar to corresponding features of an existing alert class (*See*, for example, page 6, lines 15-18 and page 7, line 13 – page 9, line 11). For example, if a new alert indicates a SYN flood attack (in which

source IP addresses are typically forged), similarity of source IP addresses might not provide a meaningful basis for comparison between the new alert and an existing alert class. Thus, when comparing the new alert to an existing alert class for correlation purposes, it may be necessary to adjust or update this similarity expectation in order to make a meaningful comparison.

The portion of Kleinman that the Examiner cites as allegedly teaching this limitation in fact only teach a method for synchronizing execution of a thread (process) to the occurrence of one or more events by grouping those events into a single "container event", and suspending execution of the thread until the first occurrence of one of these events. This is not the same as grouping alerts into classes based on similar feature values, or adjusting or updating a similarity expectation for features values of a new alert and an existing alert class. In fact, the portions of Kleinman that the Examiner cites indicate that the events in a single container event do not even have to share any similar features; one event could be the expiration of a timer and the other event could be the exit of a thread, where the occurrence of either event will suffice to unblock the suspended thread. Kleinman thus fails to teach or make obvious a method for organizing alerts in which alerts are grouped into classes based on similar feature values, and an expectation that feature values of a new alert and feature values of an existing alert class will match is adjusted or updated, as positively claimed by the Applicants in claims 6, 7 and 9. Therefore, the Applicants submit that independent claims 6, 7 and 9 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 8 depends from claim 7 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 8 is not anticipated by the teachings of Kleinman. Therefore, the Applicants submit that dependent claim 8 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

III. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Ziese in view of the Timm

patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

The Examiner's attention is directed to the fact that Ziese and Timm, singularly or in any permissible combination, fail to disclose or suggest the novel invention of transmitting information about a second sensor's belief state to a first sensor in an intrusion detection system, where the belief state indicates a state of a system resource or service and adjusting a prior belief state of the first sensor based at least in part on the second sensor's belief state, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above.

As discussed above, nowhere does Ziese teach or even suggest the desirability of adjusting a belief state of a sensor, based on a belief state of another sensor. Timm does not bridge this gap in the teachings of Ziese. Ziese and Timm, singularly or in any permissible combination, thus fail to teach or make obvious a method in which a first sensor's belief state is adjusted based on at least part of a second sensor's belief state, as positively claimed by the Applicants in claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Ziese in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

IV. INFORMATION DISCLOSURE STATEMENT

The Applicants will shortly be filing an Information Disclosure Statement in connection with the present Application. The Examiner is respectfully encouraged to review the references that the Applicants will be providing in connection with any response to this communication.

CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

11/28/05
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702